EV436703086

Substitute for form 1449B/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(use as many sheets as necessary)*	Application Number	
	Filing Date	
	First Named Inventor	Jao
	Group Art Unit	
	Examiner Name	
Sheet 1 of 2	Attorney Docket Number	MS1-1956US

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published	T[2]
/M.S./		GALBRAITH, S. D., HESS, F., SMART, N. P.; "Extending the GHS Weil Descent Attack" EUROCRYPT 2002, pgs 29-44	
		BARRETO, P. S. L. M; "The Pairing-Based Crypto Lounge" Published on the internet at http://planeta.terra.com.br/informatica/paublobarret/pblounge.html 9/13/2002, last updated 3/28/2004, 22 pgs	
		BONEH, D., GENTRY, C.; "Aggregate and Verifiably Encrypted Signatures from Bilinear Maps" Proceedings of EUROCRYPT 2003, 22 pgs	
		BONEH, D., SIVERBERG, A.; "Applications of Multilinear Forms to Cryptography" Published to the Internet at http://eprint.iacr.org 2002, 20 pages	
		BONEH, D., VENKATESAN, R.; "Breaking RSA May be Easier Than Factoring" Proceedings of EUROCRYPT 1998, 12 pages	
		BONEH, D., FRANKLIN, M.; "Identity-Based Encryption from the Weil Pairing" SIAM Journal of Computing 32, pgs 586-615	
		BONEH, D., LYNN, B., SHACHAM, H.; "Short Signatures from the Weil Pairing" Proceedings of Asiacrypt 2001, 19 pgs	
		CORON, J.-S.; "On the exact Seccurity of Full Domain Hash" Advances in Cryptology - CRYPTO 2000, 7 pages	
		FUJISAKI, E., OKAMATO, T.; "Secure Integration of Asymmetric and Symmetric Encryption Schemes" Proceedings of CRYPTO 1999, pgs 537-554	
		GALBRAITH, S. D., "Constructing Isogenies Between Elliptic Surves Over Finite Fields" Journal of Computaional Mathematics vol 2, 1999 pgs 118-138	
/M.S./		HORWITZ, J., VANKATESAN, R.; "Random Cayley Digraphs and the Discrete Logarithm" Algorithmic Number Theory Symposium, 2002, 15 pgs	

Examiner Signature	/Martinjeriko San Juan/	Date Considered	03/03/2008

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Unique citation designation number. [2] Applicant is to place a check mark here if English language Translation is attached.

Substitute for form 1449B/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT *(use as many sheets as necessary)*	Application Number	
	Filing Date	
	First Named Inventor	Jao
	Group Art Unit	
	Examiner Name	

Sheet	2	of	2	Attorney Docket Number	MS1-1956US

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
/M.S./		JOUX, A., NGUYEN, K.; "Separating Decision Diffie-Hellman from Diffie-Hellman in Cryptographic Groups" published on the internet at http://eprint.iacr.org, at least as early as March 2004, 7 pages	
		KOHEL, D.R., SHPARLINSKI, I. E.; "On Exponential Sums and Group Generators for Elliptic Curves over Finite Fields" Lecture Notes in Computer Science, 2000, pgs 395-404	
		LERCIER, R., MORAIN, F.; "Algorithms for Computing Isogenies Between Elliptic Curves" Coputational Perspectives on Number Theory: Proceedings of a Conference in Honor of AOL Atkin, 1998, 14 pgs	
		MARTIN, G.; "An Asymptotic Formula for the number of Smooth Values of a Polynomial" Journal of Number Theory, 2002, pgs 108-182	
		MILLER, V.; "use of Elliptic Curves in Cryptography" Advances in Cryptology CRYPTO 1985, pgs 417-426	
		OKAMOTO, T., POINTCHEVAL, D.; "The Gap-Problems: a New Class of Problems for the Security of Cryptorgraphic Schemes" Proceedings of the 2001 International Workshop on Practice and Theory in Public Key Cryptography, Feb 2001, 15 pgs	
		SHOUP, V.; "Lower Bounds for Discrete Logarithms and Related Problems" Revision of Paper in Proceedings in EUROCRYPT 1997, 12 pages	
		SILVERMAN, J. H.; The Arithmetic of Elliptic Curves, Spinger-Verlag, 1986 pgs 17-40, "A Survey of the Arithmetic Theory of Elliptic Curves"	
/M.S./		MAURER, U., WOLF, S.; "Lower Bounds on Generic Algorithms in Groups" EUROCRYPT 1998, 14pgs	

Examiner Signature	/Martinjeriko San Juan/	Date Considered	03/03/2008

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Unique citation designation number. [2] Applicant is to place a check mark here if English language Translation is attached.

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U. S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.